Centraal Justitieel Incassobureau
*Ministerie van Justitie en Veiligheid*

# THE FINANCIAL EMERGENCY BRAKE

CJIB app provides citizens with a GDPR-proof way to declare payment inability


Interreg
North Sea Region
BLING
European Regional Development Fund
EUROPEAN UNION

# Preface

*by Henkjan Derks*

*Henkjan Derks is Director Operations & IT at the CJIB (Central Judicial Collection Agency)*

It is estimated that nearly 1.4 million Dutch households have debt problems or face the risk of getting into debt. The extent of debt problems and its impact on people is worrying; this is why the Dutch government wants to help people to avoid, and get out of, debt.

In addressing the debt problem, the government is aiming to balance the interests of the debtor and those of the creditor. When collecting financial penalties, the social causes of debt must not be overlooked. At the same time, the government wants creditors to be more aware of the circumstances of debtors, and collect any debts owed in a socially responsible manner. This also applies to government organizations, such as the tax authorities and the CJIB.

For these reasons, the CJIB distinguishes between those people who want to pay their debts but can't, and those people in debt who are able to pay but won't. People who cannot pay a claim can now come to an agreement as to how to the debt can be paid. This helps prevent debts from arising unnecessarily. Similarly, the government also wants to avoid debts from arising in the first place wherever possible.

The CJIB uses various methods to identify people at risk of debt and to establish what measures can be taken. As a way of detecting issues at the earliest opportunity, the CJIB developed an algorithm call Debt Alert, which can predict whether someone is at risk of either going into debt or being in debt. Based on certain information, Debt Alert can predict if someone is at risk of being in debt.

When using information about past debts that have been incurred, the CJIB must and will adhere to privacy rules. As well as conforming the legal rules, the CJIB also wants citizens to have control over their information and the way it's shared. This is why the CJIB has developed the notion of the Financial Emergency Brake. This prototype has been developed in collaboration with various partners and encompasses the principles of privacy and citizen-centred sharing as described above. The Financial Emergency Brake can help with timely identification of debts. In addition, it can potentially prevent someone's debts from worsening. As such, this application contributes towards the government's wider strategy around debt reduction.

**A NOTE ON TECHNOLOGY AND BLOCKCHAIN**

All of the work described here adheres to a similar principle – technology is a means to an end, and not and end in itself. We investigate how the strengths of different technologies can help us achieve our objectives. In this case the CJIB looked for a suitable alternative to centralized or silo-ed data stores. An alternative is required which allows participating organisations to easily exchange information in a safe and legal manner, whilst maximising citizen control over their data. We call these requirements **GDPR[1]-proofing** the solution.

Blockchain was one of the technological components chosen, because of three main reasons:

1. No single partner should have control over all data – a decentralized chain of trust is required
2. Blockchain helps citizens to control their own data in a private and secure way
3. The system is more stable because there are multiple databases instead of a single point of failure

*[1] General Data Protection Regulation*

# Introduction

*by Tjitske Faber* | *Tjitske Faber is Senior Innovation Adviser at the CJIB (Central Judicial Collection Agency)*

Blockchain is a key enabling technology that will underpin efforts to deliver innovative services under the Digital Agenda for Europe. Blockchain promotes user trust by making it possible to build systems that share information and record transactions in a verifiable, secure and permanent way. Blockchain-enabled systems will allow governments to deliver a range of new solutions and service designs that have the potential to redefine the relationship between governments, citizens and SMEs in terms of transparency, trust and data-sharing. BLockchain IN Government (BLING) is part of the EU Interreg The North Sea Region Programme and builds upon the substantial investments by the EU, national governments, corporations, SMEs and wider networks to provide one of the first dedicated platforms to bring these tools and approaches into local and regional services. BLING provides a unique combination of public authorities, knowledge institutions and SMEs who will work to develop and deploy blockchain-enabled public services focusing on Identity, Direct Democracy, and Customer Services. BLING isn't a tech project: it will use and explore/enable/deliver approach to accelerate the adoption and deployment of blockchain across the NSR in order to enable the creation and delivery of the next generation of smart services for citizens, governments and SMEs.

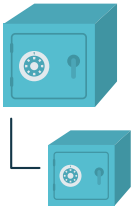
Establishing real life applications enabled by blockchain technologies, and understanding what works, why, and in what domains are the goals of this project.

BLING

- 13 partners work together on smart solutions for government service with the help of blockchain based technology
- 6 countries (NL, SWE, BEL, DEN, GER, UK)
- A consortium of knowledge partners (universities and universities of applied science), cities and regions. Each partner has a specific role in the project
- The goal of these projects is mainly to work together to get added value, so by working together and jointly developing and implementing innovative solutions for better customer services

**northsearegion.eu/bling**

The CJIB (Central Judicial Collection Agency) is one of the governmental partners of BLING and is proud to launch its first use case. In 2017 the CJIB founded an Innovationlab to find solutions for these kinds of complex issues, using a combination of data and new technologies. The Innovationlab came up with a simple but effective solution: Let's empower citizens to control the access to their personal data. The Lab then challenged the – at that point – still fairly new technology Blockchain: could this technology help make the idea sustainable and 100% GDPR-proof? And could it also be the technology which makes it easy to connect data-sources of several organizations safe and quick?



***The challenge originally resulted in the idea of a digital data safe – based on blockchain and Zero Knowledge Proof - which gives the citizens the possibility to decide for themselves which organization can see which part of their personal data.***

With funding of two parts of the Ministry of Justice (Innovation-team J&V and DGSenB) , Interreg [2], the Cyber Security Group of the Delft University of Technology (TU Delft), Ledger Leopard and Blockchainprojects.nl were able to further develop this idea, which was renamed the Financial Emergency Brake, to a sustainable new service for the Dutch Government: a cooperative framework for Citizens and Government organizations.

In this report we will get into the specifics of the Financial Emergency Brake project and show how this project can solve a problem of citizens in debt and the government have to deal with on a daily basis (chapter 1). In the following chapters we share additional information on the lessons learned regarding the security aspects (chapter 2), the developed application (chapter 3) and the legal assessment that has been conducted (chapter 4). In the closing chapter, chapter 5, we describe what are going to be to next steps for the Financial Emergency Brake project in order to implement the solution.

*[2] Interreg is a Europe-wide organisation which aims to improve national and international policy development by utilising EUR 359 million of project funding from the European Regional Development Fund (ERDF) from 2014 to 2020*

CHAPTER 01

# The CJIB Use-Case: how can government agencies exchange information that will help vulnerable citizens, whilst still complying with GDPR legislation?

*by Tjitske Faber*

*Tjitske Faber is Senior Innovation Adviser at the CJIB (Central Judicial Collection Agency)*

The CJIB enforces fines and other measures and ensures that any court-imposed penalties are collected swiftly and efficiently. If a citizen can't pay the fine in full within the specified period, the CJIB offers a service where the citizen can pay by instalments.

If a citizen doesn't pay the fine at all, or doesn't pay the full amount, they'll receive a maximum of two payment reminders. The sum payable increases with each reminder; the first reminder increases the debt to 1.5 times the original amount owing, and the second reminder increases the debt to three times the original amount owed. For example, if an initial EUR40 fine is not paid, the first reminder will increase the amount owed to EUR60. If this amount is still not paid and a second reminder is issued, the amount owing will now be EUR120.

If the citizen still doesn't pay after the second reminder, the CJIB is legally authorized to collect any outstanding fines directly from the bank account of Dutch residents. If the account number isn't available or there are insufficient funds in the account, the CJIB will instruct a bailiff to enforce collection of the debt (the citizen will also be liable for paying the costs of the bailiff).

If the bailiff is unable to recover the debt, the CJIB can apply three enforcement actions:

1. Ordering the citizen to surrender their driving licence
2. Impounding their vehicle
3. Requesting a judge to enforce the heaviest penalty in these cases - imprisonment

If this also fails and the citizen still doesn't pay, the CJIB will continue to recover the debt in forthcoming years. Not that the initial amount of the fine will have risen considerably throughout this process.

**THE WICKED PROBLEM**

The process of recovering fines is successful if everyone who receives a fine also pays it. It's the task of the CJIB to persuade citizens to pay any fines owing within the first eight weeks. However, for an increasing number of citizens, the enforcement measures don't work – **even if they wish to pay, they are unable to.** This also applies to the additional pay-by-instalments service offered by the CJIB.

To identify people who want to pay but can't, and to provide them with services and extra time to fulfil their obligations, the CJIB needs to detect some signal that the citizen is struggling with their finances or is in debt. Currently, this signal **must** be provided by the citizen themselves declaring to the CJIB that they can't pay.

The problem is, a large group of citizens feel ashamed at having to do this and are ashamed about disclosing their debt problems. Some have such high levels of debt, they feel paralysed; they do not contact the CJIB or letters from the CJIB to them are left unopened.

This group of citizens are often experiencing either harsh social conditions, mental health issues, lack the skills (such as literacy, numeracy and digital skills) needed to cope in society (or a combination of all of these).

The gravity of the debt problem often becomes apparent very late in the process, such as at the bailiff stage or even in the courtroom when a judge sees the details of the case. If the CJIB had all this information at the outset, a lot of time and money could have been saved and the debt wouldn't have snowballed, becoming a burden on both the citizen and the CJIB.

With every increase in the amount of the debt owed (due to reminders and bailiff costs), the chance of the citizen actually paying the debt decreases. The CJIB ends up trying to recover what is an excessive amount. It's not only costly for society, but it's also an irrecoverable debt and a completely inefficient process. In addition, for some citizens enforcement measures can have a devastating impact on their lives.

Over the last ten years, an increasing number of citizens have been unable to pay fines due to debt and other problems, which has become a major issue for the CJIB. The current process hinders the CJIB from collecting fines in a socially responsible way:

- By only using enforcement measures against people who refuse to pay, as opposed to people who can't pay
- Preventing the creation of additional problems for people who can't pay

## A SOLUTION: A CO-OPERATIVE FRAMEWORK FOR CITIZENS AND GOVERNMENT

Information about why citizens can't pay fines is already mostly available within the government, for example in municipalities who provide debt assistance for citizens. If this information were available to the CJIB at the outset, the CJIB would know at the very start of the process that there was no possibility that the citizen could pay the total amount within the first eight weeks.

**Now here's the problem** – because of data protection legislation, government organizations aren't permitted to share this kind of personal data.

### A Financial Emergency Brake for citizens can be a breakthrough

- A municipality knows that citizen X receives debt assistance from them. This is framed as a declaration - "citizen X receives debt assistance from the municipality"
- The declaration is passed to citizen X
- Citizen X decides (with the assistance of a social worker) whether the CJIB should be allowed to see this declaration
- If so, the framework allows the CJIB to have access to the information "Citizen X receives debt advice from the municipality". The CJIB doesn't need to access to any more detailed/less relevant financial information about citizen X - just the fact they've been receiving debt assistance.
- All the CJIB wants to know is whether citizen X can pay the fine. The fact that citizen X is receiving debt assistance is enough to indicate to the CJIB that it's highly unlikely the citizen can pay the fine.

Armed with this simple piece of information (citizen X is receiving debt assistance), it's likely that the CJIB will respond with additional services for the citizen (such as an overview of all the outstanding claims the citizen has at the CJIB, or even a customized payment proposal). This would reduce the turnaround times and the number of phone calls between debt assistance officers and the CJIB.

This solution makes the citizen the director of their own data and makes it possible to build a co-operative framework in which the citizen and the government can work together to solve current problems and prevent further ones.

Confidentiality is paramount in enabling this idea to work. It must be water-tight, no additional data should get to the CJIB if the citizen doesn't want it to. It also needs to be easy to connect to, and access, the digital data safe.

Stakeholder, like municipalities, shouldn't need to undertake a massive IT project to implement a solution such as this. It must be technically easy to connect, without using a central data warehouse.

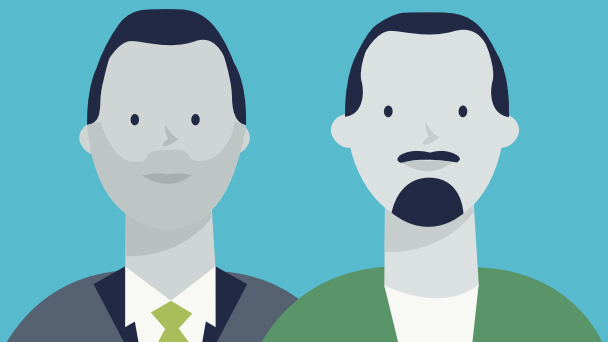
This is where Blockchain comes in, and by combining it with the concept of Zero Knowledge proofs, it transforms into a framework that can be of much more use than only the CJIB use-case.

CHAPTER 02

# Sharing privacy-sensitive data - Lessons Learned

*by Zeki Erkin and Oguzhan Ersoy*

***Zeki Erkin is Assistant Professor at Delft University of Technology (Cyber Security Group) and Radboud University Nijmegen (Digital Security Group). Oguzhan Ersoy is a PHD Student in Blockchain Technology at Delft University of Technology.***



Sharing privacy-sensitive data is at the core of the Financial Emergency Brake project. The financial status of a particular citizen is highly sensitive piece of information which should be properly protected by means of encryption and it should be strictly controlled for access. However, this information is also valuable to prevent undesired economical and legal consequences for this particular group of citizens. Hence, what is needed is a data sharing platform with privacy protection while sensitive data is not leaked.

The above scenario has two components: 1) data sharing and 2) privacy protection. Considering the first component, it is clear that the data in this platform should be provided by different organizations, e.g. several municipalities. Given that no single entity should have the complete control of the platform and every single one of them should have its ownership, the distributed ledger technology, blockchain, is the most suitable candidate to build the desired platform. The second part about preserving privacy is not only essential for GDPR compliance but also very important for the uptake of such a platform in real life. Now we will investigate these two components in details.

**DATA SHARING**

Blockchain is an append-only distributed ledger where anyone (also known as bookkeepers) in the network has the same, identical copy of the data being shared. The bookkeepers can create new piece of data (also known as blocks) based on a pre-defined protocol, such as Proof of Work, Proof of Stake, or simply Byzantine Fault Tolerant algorithms. The key point of the technology is when it is agreed, the new block is added to the chain and it is infeasible (meaning it requires exponential effort) to chance the previous blocks since they are chained one by one using cryptographic hash functions.

The above structure can be seen as a "public bulletin board" where the entities in the network can write on, and everyone can see but no one can delete or change. Thus, providing a capability which was very difficult to achieve before. Note that such a system using other techniques, e.g. websites, cannot provide same properties: ownership, integrity and transparency.

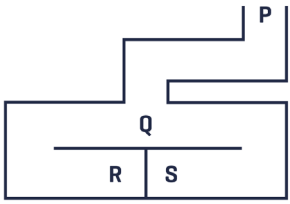
Since the Financial Emergency Brake project requires data which can be provided by municipalities, where the total number of such entities is limited, the blockchain technology with BFT algorithms are suitable to deploy. However, notice that the cryptographic construction of the blockchain technology is about append-only distributed ledger; not for privacy.

**PRIVACY PROTECTION**

The core definition of the blockchain technology is “public bulletin board” where everyone in the network has the identical data. Hence, it is not wise, even not logical, to create blocks that consist of privacy sensitive data such as financial or medical data. On one hand there is a need for sharing sensitive data and on the other hand, sensitive data cannot be shared. This dilemma can be solved by building a second layer on top of the blockchain, using cryptographic constructions, namely Zero-Knowledge Proofs (ZKPs).

**ZERO-KNOWLEDGE PROOFS**

Any claim can be proven in zero-knowledge. This means that a game can be designed between a prover and a verifier where the prover has knowledge on some claim and proves his/her claim is true without revealing this claim to the verifier. A typical example is Ali Baba’s cave.




Ali Baba’s Cave

In this game between Alice and Bob, Alice claims that she knows the magic words to open a secret gate in a cave and she needs to prove her claim to Bob, without telling the magic words to him. To achieve this goal, they play a game:

1. Bob stands outside cave and observes Alice entering the cave, without seeing which direction.
2. After Alice disappears in the cave, Bob comes to the entrance of the cave and asks Alice to come towards from one of the directions, left or right.
3. In case Alice shows from the direction that Bob asked, there are two possibilities: a) Alice was already in that part of the cave, so she was lucky. b) she was indeed on the other side, and in order to come from the right direction she needed to pass through the gate. And there is only one way for her to do so: using the magic words.

In this game above, the chance of Alice being lucky is 50%. Therefore, to convince Bob completely about the fact about Alice knowing the magic words, they need to play this game till he is convinced.

Many claims just like Alice's can also be proven in zero-knowledge by using cryptographic constructions. There are interactive games and non-interactive ones, with different computation and bandwidth requirements. Designing efficient ZKPs in terms of run-time, bandwidth and number of communication rounds has been a challenging research topics for many years.

ZKPs can be used for many claims: one can prove he/she is above 18, earns more than 50K per year, or a member of a social club. In the case of the Financial Emergency Brake project, the claim depends on the desired functionality. Claims such as:

- "Can person X pay his/her dept?"
- "Can person X pay Y Euros?"
- "Can person X pay Y Euros in Z months?"

can be designed using ZKPs. There are sufficient scientific work on ZKPs about how to provide such protocols. However, are they sufficient?

**LESSONS LEARNED**

1. There are several blockchain technologies with different properties. However, it is a matter of choice which one to use. Unfortunately, there is no unique technology that will cover different aspects: authentication, access control, secure communication, confidentiality related mechanisms etc. Therefore, there are two options: a) wait till there is a complete blockchain solution is developed (this might take some time) and b) adopt one specific blockchain technology and customize it by adding the desired components.
2. The privacy related constructions, such as ZKPS, are not mature. This is a problem in many folds: the existing research articles are very scientific, and they are not completely implemented in a ready-to-use manner. And existing implementations are very limited: using a specific language (maybe not supported by the blockchain technology of choice), provides only possibilities to prove limited number of claims. Furthermore, some of the protocols are simply not practical: they are computationally demanding and thus, not very suitable to use.

Therefore, what is needed for practical solutions for private data sharing in a distributed network is joint work between researchers and software developers, particularly on the following points:

- Development of a more complete blockchain technology with needed components,
- Secure and properly implemented, computationally efficient cryptographic protocols, such as ZKPs.

CHAPTER 03

# Explanatory note for the developed application

*by Jeroen van Megchelen*

***Jeroen van Megchelen is CTO of Ledger Leopard, an international blockchain technology company.***

We developed the CJIB solution based on Self Sovereign Identity in combination with so called Zero Knowledge Proof.

## SELF SOVEREIGN IDENTITY

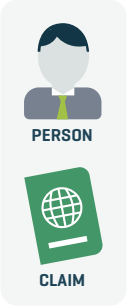
Self Sovereign Identity is the concept whereby people and businesses can store, manage and share their own identity. Data can be shared efficiently with parties that can validate it, without having to rely on a central repository of identity data. It is a digital way of doing what we do today when we hand over our paper-based driver's licence or passport as part of a verification process. Self Sovereign Identity has advantages over both current manual processes and central storage locations.

### COMPONENTS

The Self Sovereign Identity principle consists of different parts described below.

**App and wallet**

To start, the user needs an app on a smartphone or computer, and a "identity wallet" where identity data can be stored on the hard drive of the device. The identity wallet starts empty with only a self-generated identification number derived from public key, and a corresponding private key (like a password, used to create digital signatures).




**Claim**

An identity claim is an assertion from a person or company:
My name is Jeroen van Megchelen and I was born on 29/12/1980
This data is issued by a participant of the system according the appropriate schema..

**Proof**

A proof is for example, a document that provides evidence for the claim. Proofs are available in various formats. Usually for individuals it is a passport, birth certificate and invoices of companies. For companies it is a bundle of documents about incorporation and ownership structures.

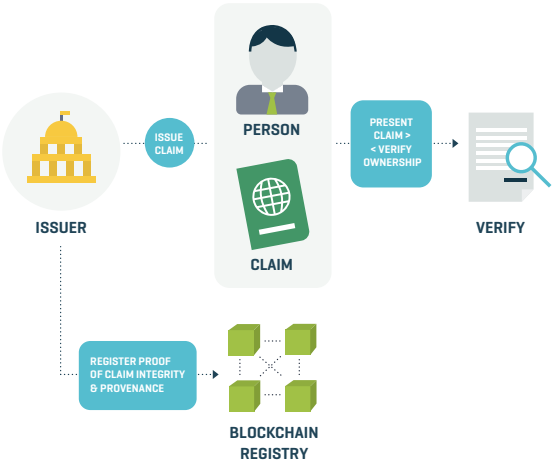

### Issuer

The claim is issued to an issuer, a known and trusted real-world entity, to be verified. The claim is send to the issuer using a secure connection. Anticipated issuers include banks, universities, hospitals, and governments, among numerous others. Within an SSI ecosystem, these established entities can provide credentials that are easily verifiable and tamper-resistant through digital signatures. The issuer can revoke claims at any time. The verified claim is send to the wallet of the user.

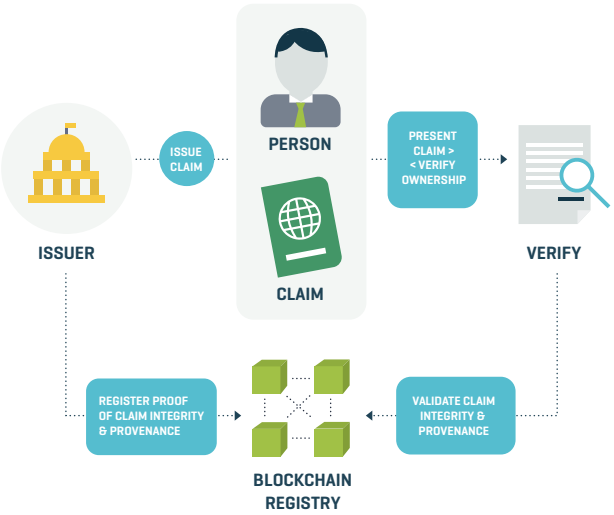
The resultant credentials will be stored in the user's wallet. The wallet is a storage system used by the SSI application to store data, keys and credentials. It is usually encrypted with some kind of PIN or master password. If another entity requires previous credentials as a proof, in order to provide other credentials, then the user can send these credentials as proof of the previous entity's internal checking process.

### Ledger

Once trusted parties issue the verifiable credentials, they can be verified by anyone because the issuer's identifier and verification key (public key) are immutably stored on the Blockchain. This means that the public key can be queried to ensure that it was, in fact, the specific entity who signed the attributes and/or message.




This proof can be verified by querying the ledger/Blockchain to ensure that the entity that supposedly issued the credential, is trusted and did indeed sign it.




**Verifier**

A verifier is a party that can check the verifiable claim presented by the person to. The verifier is able to verify the claim by both the identity holder and issuer, if the claim is valid, and if the claim hasn't been revoked.

**DID = Decentralized Identifier**

Decentralized Identifiers (DID) are self-sovereign digital identities controlled by the owner rather than a central authority. A DID record is a key-wise pair of cryptographically secure private and public keys. Pairwise identifiers create a unique identifier, or DID, for each relationship. Only you have access to the private key that could, for example, authorize access to health care data to your insurance company or KYC compliance with a cryptocurrency trading platform.

## FINANCIAL EMERGENCY BRAKE CASE DESCRIPTION

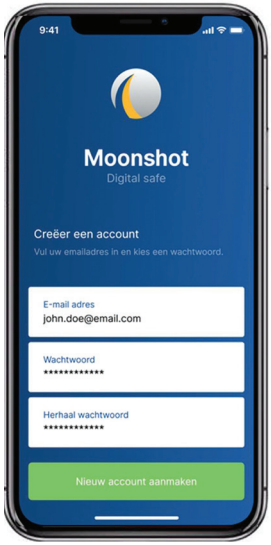
***For the CJIB case a specific app and dashboard were developed, using the Sovrin Self Sovereign Identity solution.***

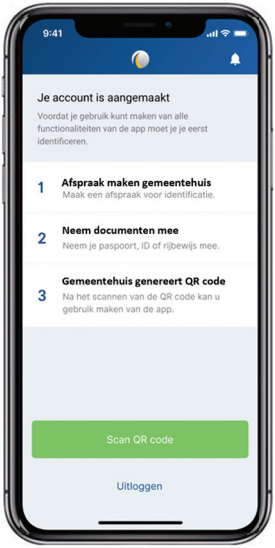
To facilitate the process, the different stakeholders take the following steps.

**STEP 1**

A citizen visits the municipality to receive a verified claim for his/her identity and a claim that he/she is in debt.

To do so, the citizen will need to download the app first and register.



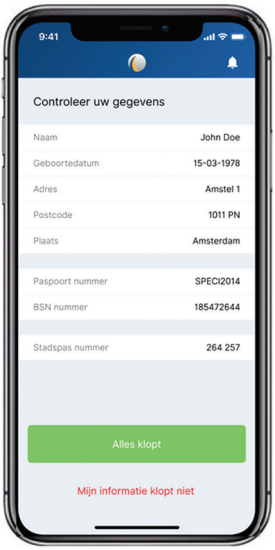




**STEP 2**

After a positive registration and activation of the app the user, an overview of the required documentation and the next steps will be displayed.

**STEP 3**

The municipality employee verifies the identification document of the citizen and the papers that proof that the citizen is in debt. When both are declared authentic by the municipality employee, the citizen will be ask to scan a QR code generated from the municipality dashboard.


**STEP 4**

After scanning the QR code, a secure connection is created and the verified claim is send to the mobile device of the citizen to be checked and stored in the wallet.

**STEP 5**

As a result of this process, the municipality and the CJIB (when given permission) can check the verified claim to determine if the citizen is in debt and receives help for this. The CJIB now knows the citizen needs additional time and/or services to prevent debt from accumulating. When the citizen is no longer in debt, he/she can revoke the claim and permissions and stop the process.

CHAPTER 04

# Legal report

*by Simon Sanders*

*Simon Sanders is attorney at law at CMS Lawyers*

**PURPOSE**

As part of the project, the application as described in the previous chapters was reviewed from a legal perspective, taking into consideration the requirements of the GDPR with respect to the use of certain Blockchain technologies. The purpose of this legal analysis was to validate whether the application processed any personal data that would in any form be stored or otherwise processed on "the blockchain" and if this would be the case, whether such processing (or any future processing) would be possible whilst meeting the requirements of the GDPR. The analysis was done by following the data flow of data submitted by the citizen from the point of data entry and looking at such aspects as data storage data exchange, and data deletion/erasure/rectification.

**THE APPLICATION**

The application itself is fairly straightforward, enabling the CJIB to obtain information on the registered debt position of a citizen (the applicant). This information – which is called a Claim - is shared between the municipality and the CJIB through a secure connection. The entities exchanging the Claim can validate whether the Claim contains all the required "authenticity features" by "calling" the blockchain. The authenticity features as are stored on the blockchain. The blockchain acts as "validator" of information and authenticity but does not store or process any actual information exchanged.

The Nodes on which the blockchain is installed, are controlled by all the participants. In summary the application consists of:

1. a web interface and an encrypted database, used by the administration to register personal information and debt position of an applicant, and issue a formal declaration (the Claim);
2. a wallet installed by the applicant on a mobile phone to receive the Claim on the phone. Wallet and Claim are linked to the applicant on the phone itself;
3. a wallet held by the municipality to store Claims for sharing with third parties if authorized by the applicant;

4. a blockchain which is used to check authenticity and validity of the so-called Schema including attributes and credential definitions which are signed by the issuing entities and a method of determining the existence of the Claim (including a mechanism verifying revocation);

**THE ANALYSES**

We made the following observations through i) interviews with the supplier of the application ii) a study of the methods used (including methods described by Sovrin) and iii) a code review (including explanation by supplier) of certain parts of the code:

1. No personal data of the applicant is stored on the blockchain itself. The blockchain only contains signed formats which are used when verifying the Claim, the existence of the Claim, but not the Claim, and authorization schemes;
2. Wallet validation will be provided by a side chain solution as a future development;
3. Only Claims connected to the Participant can be stored on the Wallet (in development);
4. All Nodes are controlled by the participating entities;
5. All data entries can be deleted or amended, either by the applicant (SSI) or through the participating entities;

**GDPR RELATED FINDINGS**

Based on the observations we have come to the conclusion that no personal data is processed on the blockchain and the rights of the data subject as set out in the GDPR can be facilitated either through the use of functionality available to the data subject (SSI) or through requests to the participants involved.

CHAPTER 05

# Next steps

*by Koen Hartog and Tjitske Faber*

***Koen Hartog is the co-initiator and program manager of blockchainprojects.nl, a blockchain program for the Dutch government. Tjitske Faber is Senior Innovation Adviser at the CJIB (Central Judicial Collection Agency).***

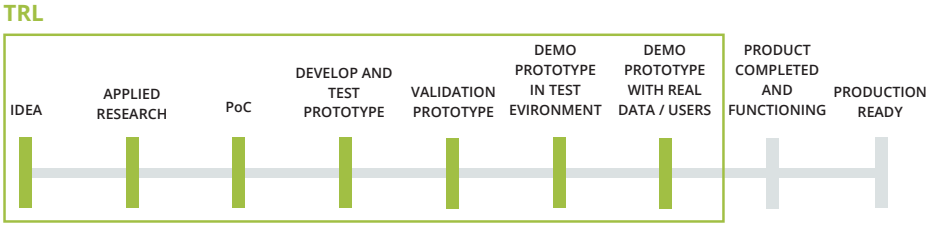
The Financial Emergency Brake project is a prime example of the heralded Triple Helix approach, a collaboration between the government, the private sector and the knowledge sector. The project team has shown that this collaboration doesn't necessarily come at the cost of slow development. The progression that has been made is impressive; we are on the verge of implementing the first legally checked governmental process including a blockchain component, self sovereign identity and zero knowledge proofs. For the final part of our project a collaboration with a limited number of municipalities is in the making. With the support of these cities we will give their citizens control over their data and solve an important societal problem.

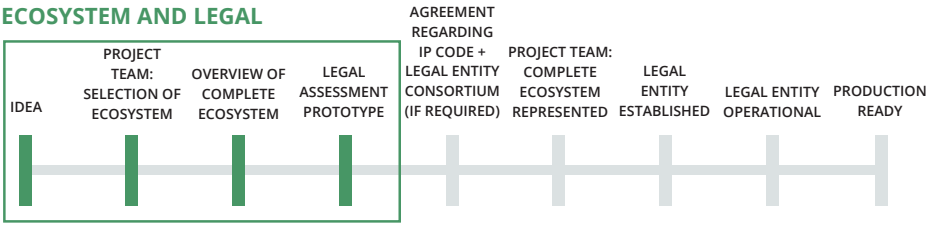
The testing phase also marks the starting point of an increase in organizational focus of the project team. CJIB and its partners from the public and private sector should agree on the legal status of the application, intellectual property (if any) and the way the application will be further developed. In other words, we need to do (more) work on governance to ensure the sustainability and continuous growth of the application.

## Timeline implementation

**TRL** = Technical Readiness Level, technical development of the system / application

**Ecosystem / Legal** = Ecosystem development and legal assessment(s) that need to take place before implementing the system / application






At the same time, we need to be mindful that the CJIB application is only the first application. In essence, CJIB's project is a first - important - application of Self Sovereign Identity by the Dutch government. Using the same building blocks (no pun intended) and methodology, we can create a multitude of privacy preserving governmental services. For example, any project where the sharing of information between organizations can benefit vulnerable citizens would be a good candidate for this type of solution.

This will be our challenge for the upcoming months and years; finishing a fully operational application which is scalable and embedded in a collaboration or consortium that can continue to expand the ecosystem. And at the same time, make the technology available for other applications that benefits citizens and the government.


northsearegion.eu/bling

Interreg
North Sea Region
BLING
European Regional Development Fund

EUROPEAN UNION